

MEL:RAS/JKW  
F. #2021R00415

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
THE BASEMENT OF 889 E. 38TH  
STREET, BROOKLYN, NEW YORK 11210  
AND ALL CLOSED AND LOCKED  
CONTAINERS AND ELECTRONIC  
DEVICES FOUND THEREIN

TO BE FILED UNDER SEAL

APPLICATION FOR A  
SEARCH WARRANT FOR A PREMISES  
AND ELECTRONIC DEVICES FOUND  
THEREIN

Case No. 22-MJ-254

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Brian G. Gander, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as the basement of 889 E. 38th Street Brooklyn, New York 11210 and all closed and locked containers and electronic devices found therein, hereinafter the “SUBJECT PREMISES,” further described in Attachment A, for the things described in Attachment B.
2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since approximately September 2002. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to

request a search warrant. I am part of the Child Exploitation and Human Trafficking Task Force with the FBI and New York City Police Department (the “Task Force”). I have extensive experience investigating cases relating to sex trafficking and sex trafficking of minors. I have experience executing search warrants, including search warrants relating to the search of a premises and electronic devices found therein.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. On or about March 7, 2022, a grand jury sitting in the Eastern District of New York returned a four-count indictment, charging ELIJAH WUSU, also known as “Lucky,” with one count of sex trafficking conspiracy between March 2019 and September 2021, and three counts of sex trafficking, including one count of sex trafficking of a minor, in violation of Title 18, United States Code, Sections 1591 (sex trafficking) and 1594 (conspiracy to commit sex trafficking). See, 22-CR-95 (DLJ), ECF No. 1 (the “Indictment”). In addition, there is probable cause to believe violations of Title 18, United States Code, Sections 2251 (sexual exploitation of a minor), 2252 (child pornography offenses),<sup>1</sup> 2421 (the Mann Act) and 2422 (coercion and

---

<sup>1</sup> The terms “minor,” “sexually explicit conduct,” “visual depiction” and “child pornography” are defined as set forth in Title 18, United States Code, Section 2256.

enticement) (together with the offenses charged in the Indictment, the “Subject Offenses”) have been committed by WUSU and others known and unknown. On or about March 7, 2022, a warrant was issued for WUSU’s arrest. Based on the facts set forth in this affidavit, there is probable cause to believe WUSU and others committed violations of the Subject Offenses. There is also probable cause to search the SUBJECT PREMISES described in Attachment A for evidence of the Subject Offenses as further described in Attachment B. The Task Force anticipates executing the requested warrant of the SUBJECT PREMISES in conjunction with the arrest warrant issued in connection with the Indictment.

#### **THE SUBJECT PREMISES**

5. The SUBJECT PREMISES is the basement of 889 E. 38th Street, Brooklyn, New York 11210. The SUBJECT PREMISES is the basement of a single family townhouse with gray and white siding. The front entrance to the house is a grey door behind a second glass door with steps leading up to the entrance that are surrounded by a red brick wall. The door to the basement, or the SUBJECT PREMISES, is a grey metal door that lifts up with steps leading down into the SUBJECT PREMISES. While this affidavit only seeks to search the basement of the residence, it seeks authority to enter the SUBJECT PREMISES through both the front door of the house, which will require law enforcement officers to walk through a portion of the house not subject to the warrant, as well as the back door leading directly to the SUBJECT PREMISES.

This request is made to ensure officer safety while effectuating the search warrant and anticipated arrest. Pictures of the exterior of the SUBJECT PREMISES are below:



6. WUSU is on New York State probation and lists the SUBJECT PREMISES as his address with his probation officer. Probation officers last visited the SUBJECT PREMISES on February 12, 2022, and WUSU was present. Based on victim reports, WUSU resides in the basement of the house and his mother and sister reside upstairs. Accordingly, this search warrant application seeks authorization to search all parts of the SUBJECT PREMISES, which consists

of the basement of the house located at 889 E. 38th Street, Brooklyn, New York, and all closed and locked containers and electronic devices found therein, for the things described in Attachment B.

### **PROBABLE CAUSE**

#### **I. Background**

7. Since at least February 2020, the Task Force has been investigating ELIJAH WUSU, also known as “Lucky,” for the Subject Offenses. As part of its investigation, the Task Force has, inter alia, reviewed online advertisements for commercial sex, interviewed victims and obtained information from the Internet and communications providers. As set forth in more detail below, there is probable cause to believe that WUSU and others caused at least four victims to engage in commercial sex acts (hereinafter, “Victim-1,” “Victim-2,” “Victim-3” and “Victim-4”), including by violence and threats of violence, and that WUSU received financial benefit from his victims’ sex acts. Victim-3 was a minor during the relevant time period.

8. WUSU also attempted to entice another minor, Victim-5 (together with Victim-1, Victim-2, Victim-3 and Victim-4, the “Victims”), to engage in prostitution on his behalf, although she did not ultimately work for him. Four of the victims, who are referred to herein as Victim-1, Victim-2, Victim-4 and Victim-5, were recruited on Facebook to work for WUSU.

## II. Victim-1

9. In or about March 2019, an adult victim, Victim-1, received a Facebook message from a user named “Vida Kashh” recruiting Victim-1 to work for WUSU.
10. Records from the Vida Kashh Facebook account, obtained through a judicially authorized warrant, show that in or about March 2019, Vida Kashh contacted Victim-1 and advised Victim-1 that Vida Kashh did “dates,” advised Victim-1 that she was “hiring ladies,” and provided Victim-1 with a phone number for “Lucky” and directed Victim-1 to call Lucky. The registration email address associated with the Vida Kashh Facebook account is chaseeachek@yahoo.com. This email address is on file with the New York State Probation Department for WUSU.
11. Based on my training and experience, as well as my participation in this investigation, I understand the term “date” to refer to a meeting for the purpose of engaging in commercial sex.
12. Shortly after receiving Lucky’s phone number, Victim-1 called Lucky, who she subsequently identified in a photograph as being WUSU. WUSU told Victim-1 that he would take care of Victim-1 if Victim-1 went on “dates,” which Victim-1 understood to mean engage in prostitution. Victim-1 agreed. WUSU then provided Victim-1 with another phone number to call him and paid for a cab to bring Victim-1 to WUSU’s residence in Brooklyn.
13. Thereafter, Victim-1 resided with WUSU at his residence in Brooklyn while Victim-1 engaged in commercial sex acts on WUSU’s behalf. According to Victim-1, she and



WUSU resided in the basement of a house in Brooklyn, and WUSU's mother and sister lived in the rest of the house. Victim-1's description of WUSU's residence is consistent with the SUBJECT PREMISES.

14. Victim-1 worked for WUSU in or about and between March and April 2019 and communicated regularly with WUSU by cellular telephone. WUSU advised Victim-1 that he wanted to bring her out-of-state to engage in prostitution.
15. When Victim-1 began working for WUSU, the walls of WUSU's room were white and blue and the floor was concrete. However, shortly after she began working for WUSU, he painted the walls green and put brown carpet on the floor. Images of Victim-1 and WUSU sent from Victim-1 to WUSU in or about May 2019, were recovered pursuant to a judicially authorized warrant from WUSU's Facebook account with vanity name Luciano Gallucio. In one such picture, Victim-1 and WUSU appear in front of a bright green wall (the "Green Wall"). The Luciano Gallucio account lists under "Employeeer [sic] Description," "break a hoe university."
16. At WUSU's direction, Victim-1 engaged in "out calls," which means that she would travel to customers' residences or hotel rooms to engage in commercial sex acts. WUSU also had Victim-1 work out of hotel rooms approximately two times per week and arranged "car dates," where she would engage in commercial sex acts in cars. WUSU paid for hotel rooms on at least one occasion.

17. WUSU had multiple cellular telephones, which he used to communicate with customers and victims.
18. WUSU bought boxes of condoms, which Victim-1 used with customers. Victim-1 had approximately six to seven customers per day. At WUSU's direction, Victim-1 charged customers between \$90 and \$200 depending on the sex acts involved and length of the interaction. When Victim-1 met with a customer, the customer paid Victim-1. At the end of the night, Victim-1 gave the money earned that day to WUSU, and WUSU gave Victim-1 a portion of the proceeds. Based on text communications between WUSU and Victim-1, I know that some customers paid through Cash App, which is an application used on electronic devices that allows for the electronic transfer of money.
19. WUSU was violent with Victim-1 on several occasions. On one occasion, WUSU began beating Victim-1 while Victim-1 was asleep after WUSU went through Victim-1's phone and became angry about text messages exchanged between Victim-1 and a male. On another occasion, Victim-1 tried to leave WUSU's apartment to go home. Victim-1 relayed to law enforcement that when she left WUSU's apartment that day, she did not intend to return and did not intend to continue working for WUSU. After Victim-1 left WUSU's residence, WUSU followed her outside, grabbed Victim-1 by the neck and choked Victim-1 until she fainted.
20. Victim-1 worked for WUSU for approximately three weeks before leaving WUSU's residence. During that time, and at WUSU's direction she got a tattoo of his alias, "Lucky," on her body. In order to safely leave WUSU's residence, Victim-1 provided WUSU



with a false story about where she was going and indicted that she would return to WUSU's residence. After Victim-1 left WUSU's residence, WUSU contacted Victim-1 by phone and text, cursing at her because he wanted her to come back and make money. Victim-1 has not seen WUSU since she left.

III. Victim-2

21. Based on my conversations with witnesses and law enforcement agents and my review of other evidence, I have learned that Victim-2 engaged in prostitution for WUSU intermittently between approximately 2019 and September 2021.
22. WUSU was extremely violent towards Victim-2 and assaulted her on multiple occasions, grabbing her neck and punching her.
23. On March 29, 2021, WUSU was arrested for assaulting Victim-2 at John F. Kennedy International Airport. The incident was capture on video surveillance, which I have viewed. According to a witness, WUSU punched, hit, choked and bit Victim-2's face. I have viewed photographs of Victim-2's injuries from the assault, including an image in which Victim-2 appears to have deep bite marks on her face.
24. Between 2019 and September 2021, Victim-2 appeared in numerous escort advertisements posted by telephone numbers that have been tied to WUSU. In some of these advertisements, Victim-2 is depicted in front of the Green Wall.
25. Telephone records obtained pursuant to a judicially authorized search warrant permitting a search for location information and toll records associated with a phone number

identified as the defendant's personal cellphone (347-372-1561) (the "Defendant's Phone"), see 22-MJ-213, show in February 2022, 14 calls between a telephone number associated with Victim-2 and the Defendant's Phone. When working for WUSU, Victim-1 and Victim-4 communicated with WUSU using the telephone number associated with the Defendant's Phone.

IV. Victim-3

26. Victim-3 was trafficked by WUSU and his associate ("CC -1") when Victim-3 was 17 years old.

27. In or about March 2019, Victim-1 introduced Victim-3 to WUSU and CC-1. WUSU and CC-1 directed Victim-3 to engage in prostitution and coordinated dates for Victim-3.

28. Both WUSU and CC-1 met Victim-3 in person at WUSU's residence before directing her to engage in prostitution. Victim-3 reported that WUSU resided in a basement in Brooklyn and that his room was green. Victim-3's description of the residence is consistent with the SUBJECT PREMISES.

29. WUSU organized "dates" for Victim-3, communicating with customers by cellular telephone to arrange meetings.

30. Victim-3 engaged in car dates or outcalls and gave all of the money she made engaging in prostitution to CC-1.

V. Victim-4

31. In or about January 2020, an adult victim, Victim-4, received a Facebook message from the Vida Kashh account recruiting Victim-4 to work for WUSU.
32. Records obtained from the Vida Kashh Facebook account show that in or about January 2020, the Vida Kashh Facebook account contacted Victim-4 and asked her to “trap with [Vida Kashh’s] team.” Vida Kashh then provided Victim-4 with a phone number to contact WUSU who Victim-4 subsequently identified in a photograph. Victim-4 then spoke with WUSU and, a day or two later, went to WUSU’s residence in Brooklyn.
33. Shortly thereafter, Victim-4 began engaging in prostitution for WUSU, doing car dates and out calls.
34. Victim-4 was required to pay WUSU a fee to be part of his “team.” She worked every day for WUSU for two to three months seeing approximately ten customers per day and earning approximately \$2,500 per day, all of which was turned over to WUSU.
35. WUSU handled the communications with customers via cellular telephone and Victim-4’s image was posted in escort advertisements on various websites between February and April 2020. Some of the photographs used in the escort advertisements depict Victim-4 in front of the Green Wall.
36. Victim-4 was aware that WUSU was violent with other girls and had observed injuries to Victim-2’s face after an instance in which WUSU assaulted Victim-2. In one instance, WUSU told Victim-4 that he was going to “smack the shit out of” her. WUSU told

Victim-4 that she was not permitted to look at or talk to other males and directed her on multiple occasions to stay in pocket. Based on my training, experience and involvement in this and other sex trafficking investigations, I have learned that “stay in pocket” refers to working exclusively for one particular pimp and is intended prevent a victim from being recruited by other pimps.

37. WUSU took Victim-4’s birth certificate and identification documents which

Victim-4 never recovered.

38. Victim-4 described WUSU’s residence in Brooklyn as a house. She advised that he lives in the basement and his mother and sister live upstairs. His room is green. Victim-4’s description of WUSU’s residence is consistent with the SUBJECT PREMISES.

VI. Victim-5

39. When Victim-5 was 17 years old an account with username “Luciano Gallucio (Forever Curlz)” (the “LGFC Account”) attempted to recruit her to engage in prostitution. The user of the LGFC Account identified himself in his communications with Victim-5 as “lucyy,” which I understand to be an alternate spelling of “Lucky,” which is WUSU’s alias.

40. Victim-5 used Victim-5’s Facebook account to communicate with the LGFC Account in September and October 2018, when Victim-5 was a minor. The LGFC Account initiated the conversation and asked Victim-5, “U about getting cash”?

41. At the outset of the communications, Victim-5 repeatedly stated that she was 17 years old.

42. Through September and October 2018, the user of the LGFC Account repeatedly asked Victim-5 to engage in commercial sex work, and Victim-5 repeatedly declined. For example, on or about October 13, 2018, the user of the LGFC Account stated in writing and audio messages, “U gonna be a paid bitch” and “we gonna get some money with that kitty you hear me? We gonna break them tricks you hear me?” Victim-5 responded, “I already told you . . . you’re not pimping me.” She further stated, “BOY I’M NOT SELLING PUSSY FOR YOU TF.” Based on my training and experience, as well as my participation in this investigation, I understand the term “tricks” to refer to a customer who pays another individual to engage in a sex act; I understand the term “kitty” to refer to the victim’s vagina; and I understand the foregoing statements to reference Victim-5 engaging in sex for money.
43. On or about October 14, 2018, the user of the LGFC Account sent an audio message to Victim-5’s Account that stated, “this thing right here, this is a producible thing. When you with me it’s diamonds and furs and cars and houses.” Based on my training and experience, as well as my participation in this investigation, I understand the user of the LGFC Account to be promising to provide valuable goods to Victim-5 if she engaged in commercial sex work for him.
44. Victim-5 also reported to law enforcement that she sent nude photographs of herself to the LGFC Account when she was a minor.

VII. Additional Victims

45. Law enforcement is aware of several other potential victims who worked for WUSU. Law enforcement has identified numerous phone numbers associated with WUSU that have posted escort advertisements on various websites since at least February 2018. Many of the escort advertisements depict girls or women in front of the Green Wall identified by victims as being located at the SUBJECT PREMISES. Many of these escort advertisements depict girls or women other than the victims identified herein. Law enforcement has identified numerous phone numbers and email addresses associated with those escort advertisements. The most recent advertisement associated with the defendant and identified by law enforcement was posted in September 2021.

46. Information obtained through the Vida Kashh Facebook account also indicates that there were numerous victims other than those identified herein. The account was regularly used to recruit other Facebook users to engage in prostitution and regularly referred other users to WUSU.

VIII. Probable Cause for the Search of the SUBJECT PREMISES

47. There is probable cause to believe that there is evidence of the Subject Offenses at the SUBJECT PREMISES.

48. As set forth above, there is probable cause to believe that WUSU has been engaged in the Subject Offenses since at least 2018. Victim-1, Victim-2, Victim-3 and Victim-4 reported working from the basement of WUSU's residence, which has been identified as the

SUBJECT PREMISES. The SUBJECT PREMISES is listed as WUSU's address with the New York State Probation Department and he was observed to be physically present at the address as recently as February 12, 2022 during a probation visit.

49. Moreover, extractions from WUSU's social media accounts, victim phones and WUSU's messaging applications further prove that WUSU resides at the SUBJECT PREMISES and engages in the Subject Offenses from the SUBJECT PREMISES. Specifically, the two most used IP addresses associated with the Vida Kashh Facebook account between October 29, 2019 and April 9, 2020, as well as between April 3, 2021 and May 19, 2021, are associated with the

SUBJECT PREMISES.

50. In communications between Victim-4 and WUSU recovered from Victim-4's electronic device, there are messages in which WUSU directs Victim-4 to meet him at an address on 38th Street that is one block away from the SUBJECT PREMISES.

51. WUSU provided an address located across the street from the SUBJECT PREMISES to individuals associated with WUSU's sex trafficking, including customers. For example, in or about March 2020, an undercover officer arranged a car date with a phone number associated with WUSU and was provided the address across the street from the SUBJECT PREMISES. An identified victim met the undercover and was taken into custody at that time.

52. In communications between WUSU and an unidentified individual who was using one of the telephone numbers associated with WUSU's escort advertisements, WUSU indicates



that he is on 38th Street between Glenwood Road and Avenue H, which is the location of the

SUBJECT PREMISES.

53. Based on my training and experience, as well as my participation in this investigation, I know that individuals involved in the Subject Offenses often retain documents related to sex trafficking and prostitution, including records of proceeds earned and contact information for brothels, delivery drivers, customers or other prostitution businesses. I have further learned that sex trafficking organizations often keep such records in secure locations that are easily and quickly accessible.

54. Based on my training and experience, as well as my participation in this investigation, I know that individuals involved in the Subject Offenses often keep condoms, lubricants, lingerie, high-heeled shoes, wigs and other materials related to prostitution for use by the women and girls who work for them.

55. In addition, there is probable cause to believe that any electronic devices found at the SUBJECT PREMISES will contain evidence of the Subject Offenses. As set forth in detail above, WUSU and his co-conspirators used electronic devices to conduct the sex trafficking operation. Since at least February 2018, WUSU has been associated with hundreds of escort advertisements online. WUSU also used electronic devices to communicate with customers and his victims; he used social media platforms such as Facebook to recruit victims; and he accepted payment for commercial sex services through electronic applications such as Cash App.

56. In addition, as set forth above, WUSU directed at least one victim, who was under the age of 18 to send him sexually explicit images. Based on my training, experience and participating in the investigation, I know that individuals who collect sexually explicit images and videos of minors often store and maintain those images on electronic devices or social media accounts.

57. Accordingly, there is probable cause to believe that any electronic devices at the SUBJECT PREMISES will contain evidence of the Subject Offenses. At this time, however, this application only seeks authority to seize all electronic devices found at the SUBJECT PREMISES, and seeks authority to search only those devices found on WUSU's person, found in WUSU's immediate vicinity and/or with telephone number 347-372-1561.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

58. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, including on cellular telephones, or other storage media. Thus, the warrant applied for would authorize the seizure of certain electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

59. *Probable cause.* I submit that if a computer or storage medium, including cellular telephones, is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet, including files viewed using a cellular telephone, are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of other evidence related to this investigation, I am aware that electronic equipment was used in the commission of the Subject Offenses.

60. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the

SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).  
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times a device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the device or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether a device was remotely accessed, thus inculcating or exculpating the device owner. Further, computer and storage media activity can indicate how

and when a device or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with a device, and the IP addresses through which a device accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate a device user. Last, information stored within a computer may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within a device may indicate the owner's motive and intent to commit a crime

(e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the relevant device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the device and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence



of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

61. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of a device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

62. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing of all electronic devices found at the SUBJECT PREMISES (the “Subject Devices”), and seizing, imaging, or otherwise copying storage media from electronic devices that are found on WUSU’s person, that are found in WUSU’s immediate vicinity and/or with telephone number 347-372-1561 (the subset of devices subject to search are defined herein as the “Searchable Devices”), and would authorize a later review of the media or information from the Searchable Devices consistent with the warrant.

The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### **BIOMETRIC UNLOCK**

63. The electronic devices recovered at the SUBJECT PREMISES may include smartphones or other electronic devices that offer their users the ability to unlock the device via the use of biometric data in lieu of a numeric or alphanumeric passcode or password, including the person's facial features (*e.g.*, on devices manufactured by Apple, Inc. ("Apple"), including iPhones, a common feature of this type called "Face ID" that scans a person's face using the smartphone's camera and unlocks the device for recognized users) or fingerprint (*e.g.*, a feature on Apple devices similar to Face ID called "Touch ID," which unlocks the device in response to a recognized finger or thumbprint).<sup>2</sup>

64. In some circumstances, biometric data cannot be used to unlock a device that has such identification features enabled, and a passcode or password must be used instead. These

---

<sup>2</sup> In the course of my training and experience, I have become familiar with federal court decisions standing for the proposition that government agents may compel individuals to provide biometric data in order to effectuate a search of devices lawfully seized pursuant to a warrant. For example, in In re Search Warrant Application, 279 F. Supp. 3d 800, 801 (N.D. Ill. 2017), a district court in the Northern District of Illinois reversed a magistrate judge's decision that the Fifth Amendment's privilege against self-incrimination barred a portion of a search warrant that would have required "residents of a home to apply their fingers and thumbs (as chosen by government agents) to the fingerprint sensor on any Apple-made devices found at the home during the search." The district court noted that the Fifth Amendment "only prevents

circumstances may include, for example, when (a) a device has been turned off or restarted; (b) the device has received a remote lock command; (c) more than forty-eight hours have passed since the last time the device was unlocked; (d) when the device has not been unlocked via the feature within a certain period of time; or (e) multiple unsuccessful attempts to unlock the device via such features are made. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device biometric identification features often exists only for a short time.

65. In my training and experience, users of devices that offer biometric identification features often enable them because they are considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect a device's contents. This is particularly true when the user(s) of the device

---

the government from compelling a person from being a 'witness' against himself" and that, since "[w]itnesses provide *testimony*, [ ] that is the forbidden compulsion; the government cannot force someone to provide a communication that is 'testimonial' in character." *Id.* at 803 (emphasis in original). On the other hand, "the Supreme Court has distinguished between compelling a communication versus compelling a person to do something that, in turn, displays a physical characteristic that might be incriminating." *Id.* (citing *United States v. Hubbell*, 530 U.S. 27, 34 (2000), and collecting cases). Applied in the context of biometric data, the court held that, especially where government agents select the fingers to be pressed on the Touch ID sensor, thereby eliminating the "need to engage the thought process of any of the residents at all in effectuating the seizure," "[t]he application of the fingerprint to the sensor is simply the seizure of a physical characteristic, and the fingerprint by *itself* does not communicate anything." *Id.* at 803-04 (emphasis in original). Similar reasoning supported a search warrant that would compel biometric data not only from an individual's fingerprints but from his face and irises as well. See *In re Search of [Redacted Text]*, Case No. 18-SW-0122 (GMH), 2018 U.S. Dist. LEXIS 109572 (D.D.C. June 26, 2018).

are engaged in criminal activities, and thus have heightened concerns about securing the contents of a device.

66. The passwords or passcodes that would unlock electronic devices recovered at the scene are not known to law enforcement. As such, it likely will be necessary to scan the face of a user of such devices or press the fingers of the user to the device's biometric sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant.<sup>3</sup> Attempting to unlock such devices in this manner is necessary because the law enforcement may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

67. In light of the foregoing, I request that the Court authorize law enforcement to hold WUSU in place in front of any Searchable Devices falling within the scope of this warrant in order to activate the Face ID unlock feature, and/or press the fingers (including thumbs) of

---

<sup>3</sup> Although it is unknown which of a given user's fingerprints may be capable of unlocking a particular device, based on my training and experience, I know that it is common for users to unlock their devices via the fingerprints on their thumb or index fingers. In the event that law enforcement is unable to unlock a seized device as described above within the number of attempts permitted by the device, it will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

WUSU to the biometric sensors of any such devices, in order to search their contents as authorized by this warrant.

**CONCLUSION**

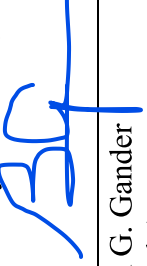
68. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

**REQUEST FOR SEALING**

69. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Premature disclosure of the

contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



---

Brian G. Gander  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone  
on March 8th, 2022

*Taryn A. Merkel*

---

HONORABLE TARYN A. MERKL  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK



## **ATTACHMENT A**

### *Property to be searched*

1. The property to be searched is the basement of 889 E. 38th Street, Brooklyn, New York 11210, further described as the basement of a single family townhouse with gray and white siding. The front entrance to the house is a grey door behind a second glass door with steps leading up to the entrance that are surrounded by a red brick wall. The door to the basement, or SUBJECT PREMISES, is a grey metal door that lifts up with steps leading down into the SUBJECT PREMISES. For the safety of officers effectuating the search warrant, law enforcement officers may enter the SUBJECT PREMISES through both the front door of the house, which will require law enforcement officers to walk through a portion of the house not subject to the warrant, as well as the back door leading directly to the SUBJECT PREMISES.

Pictures of the exterior of the SUBJECT PREMISES are below:



**ATTACHMENT B**

*Property to be seized*

1. All evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1591 (sex trafficking of a minor or by force, fraud, or coercion), 1594 (conspiracy to commit sex trafficking), 2251 (sexual exploitation of a minor), 2252 (child pornography offenses), 2421 (the Mann Act) and 2422 (coercion and enticement) (the “Subject Offenses”) have been committed by ELIJAH WUSU, also known as “Lucky,” and others known and unknown, occurring on or after February 1, 2018, including:
  - a. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
  - b. Evidence concerning the identities or locations of prostitution customers, victims of the Subject Offenses or co-conspirators involved in the Subject Offenses, including without limitation, mail matter, physical or electronic records or data associated with customer transactions, notes, address books, and photographs.
  - c. Evidence concerning the establishment or management of a sex trafficking organization or prostitution business, including without limitation, documents and other records relating to advertising men, women and/or girls for prostitution.

- d. Communications, including but not limited to letters, phone calls, emails and text messages, between WUSU, victims, customers and/or other current or former co-conspirators related to the Subject Offenses;
- e. Records and information relating to the Subject Offenses, including but not limited to prostitution earnings contact lists and telephone numbers, e-mail accounts and Facebook accounts utilized by WUSU in connection with the Subject Offenses;
- f. Computers, smart phones, tablets, or other computer devices and storage media.  
Law enforcement may seize all electronic devices found at the SUBJECT PREMISES (the “Subject Devices”) and may search any such devices found on WUSU’s person, found in WUSU’s immediate vicinity and/or with telephone number 347-372-1561 (the subset of devices subject to search are defined herein as the “Searchable Devices”) in a manner consistent with this warrant;
- g. Computerized or written books, records, receipts, notes, ledgers, money orders, calendars, address books, customer lists, travel records and other documents related to the Subject Offenses;
- h. U.S. currency, money transmitter receipts, wire transfer records, bank account information, cash transfer applications and other records detailing the receipt and sending of U.S. currency;
- i. Precious metals, jewelry or other forms of illicit proceeds;

- j. Photographs and videos related to the Subject Offenses;
- k. Condoms, lubricants, lingerie, high-heeled shoes, wigs or other materials related to sex trafficking or prostitution;
- l. Records, keys and passcodes concerning cabinets, storage lockers, safety deposit boxes, suitcases, briefcases, safes, key-lock strong boxes and other types of locked or closed containers;
- 2. For any computer or storage medium, including cellular telephones, whose seizure is otherwise authorized by this warrant and which is found on WUSU's person, found in WUSU's immediate vicinity and/or is a device with telephone number 347-372-1561, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (the Searchable Devices):
  - a. evidence of who used, owned, or controlled the Searchable Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the Searchable Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the Searchable Devices was accessed or used to determine the chronological context of Computer access, use, and events relating to crime under investigation and to the Searchable Devices user;
- e. evidence indicating the Searchable Devices user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the Searchable Devices of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Searchable Devices;
- h. evidence of the times the Searchable Devices was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the Searchable Devices;
- j. documentation and manuals that may be necessary to access the Searchable Devices or to conduct a forensic examination of the Searchable Devices;
- k. records of or information about Internet Protocol addresses used by the Searchable Devices;

1. records of or information about the Searchable Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes law enforcement personnel to:

1. Press or swipe the fingers (including thumbs) of Elijah WUSU to the fingerprint scanner of any Searchable Device with a biometric unlocking feature;
2. Hold Elijah WUSU in place while holding a Searchable Device with a biometric unlocking feature in front of his face to activate the facial recognition feature; and/or
3. Hold Elijah WUSU in place while holding a Searchable Device with a biometric unlocking feature in front of his face to activate the iris recognition feature, all for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Law enforcement officers or agents will select which fingers to press to the Searchable Device(s).

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of certain electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.